Abstract

A method of and system for encrypting and decrypting data on a computer system is disclosed. In one embodiment, the system comprises an encrypting operating system (EOS), which is a modified UNIX operating system. The EOS is configured to use a symmetric encryption algorithm and an encryption key to encrypt data transferred from physical memory to secondary devices, such as disks, swap devices, network file systems, network buffers, pseudo file systems, or any other structures external to the physical memory and on which can data can be stored. The EOS further uses the symmetric encryption algorithm and the encryption key to decrypt data transferred from the secondary devices back to physical memory. In other embodiments, the EOS adds an extra layer of security by also encrypting the directory structure used to locate the encrypted data. In a further embodiment a user or process is authenticated and its credentials checked before a file can be accessed, using a key management facility that controls access to one or more keys for encrypting and decrypting data.